UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

DAVID STERLING, an Individual and STERLING & STERLING,I NC., a corporation on behalf of themselves and others similarly situated,

Plaintiffs,

v.

STRATEGIC FORECASTING, INC. and GEORGE FRIEDMAN

Defendants.

----------X

CV12 - 297

LINDSAY, J.
BISLEY, J.

COMPLAINT

JURY TRIAL DEMANDED

SUMMONS ISSUED

Plaintiffs DAVID STERLING ("Sterling") and STERLING & STERLING, INC. (hereinafter "S&S" or "Sterling & Sterling, Inc." and collectively, "Plaintiffs") bring this class action complaint on behalf of themselves and all others similarly situated (the "Class"), upon knowledge as to the facts and upon information and belief as to all other matters, based on the investigation of their counsel, NAPOLI BERN RIPKA SHKOLNIK, LLP, against defendants STRATEGIC FORECASTING, INC. ("Stratfor") and GEORGE FRIEDMAN (hereinafter "Friedman" and collectively with Stratfor, "Defendants") and state as follows:

I. Nature of the Action

1. This is a consumer class action for damages arising from Defendants' failure to secure its computer storage systems to protect Stratfor's users', subscribers', and those persons and entities that provided Stratfor with personal and financial information ("Customers"). Defendants also failed to timely notify Stratfor's Customers of their security breach until the unidentified third-parties who accessed Defendants computer storage systems notified the public on December 24, 2011.

2. Defendants keep and maintain a database of all Stratfor's Customers who provide Defendants with personal and financial information. Stratfor also maintains emails and communications they have with Customers on their servers. Stratfor did not encrypt or protect information provided by Customers to the company. Defendants' lax security measures allowed third-parties to access Defendants' computer storage systems at will and access any information desired.

3. In early December 2011, and on an exact date known only by Defendants, Defendants learned that a third-party, without authorization, obtained, disclosed, and utilized personal and financial information from Stratfor users and destroyed Stratfor's servers. Defendants kept their knowledge of the security breach secret from the public and did not alert its Customers until approximately December 28, 2011, and only after the third-parties had already disclosed to the public that they had succeeded in accessing Defendants' computer storage systems.

4. As a result of Defendants' failure to secure its systems and notify Plaintiffs and all members of the proposed Class of the theft of their personal and financial information, Plaintiffs and members of the proposed Class suffered and were caused injuries including: the financial expenses associated with third-party use of credit card and other financial information; the expense of securing replacements of compromised credit card numbers, online passwords, and the employment of monitoring services to protect against fraud; the deprivation of an opportunity to safeguard personal and financial information, monitor credit card activity, and take steps to prevent identity theft due to Defendants delayed notification to the public; exposure to computer viruses targeting corporations, individuals, and other entities using the email addresses and personal information obtained; embarrassment and invasion of privacy due public exposure of private email communications; loss of use of the Stratfor website that Plaintiffs and members of

the proposed Class paid subscription fees to access.

5. In this action, Plaintiffs seek to recover damages, equitable, and other relief available, from Defendants, on behalf of all Customers of Defendants' services.

II. Parties, Jurisdiction, and Venue

6. Plaintiff David Sterling is a citizen of the State of New York.

7. Plaintiff Sterling & Sterling Inc. is corporation existing and organized under the laws of the State of New York, whose principal place of business is 135 Crossways Park Drive, Suite 300, Woodbury, NY 11797 and whose business is in the insurance brokerage industry.

8. Defendant Strategic Forecasting, Inc. is a corporation existing and organized under the laws of the State of Texas whose principal place of business is 221 West 6th Street, Suite 400 Austin, TX 78701 and whose business is analyzing and publishing global news online to and via email to subscribers.

9. Defendant George Friedman is a U.S. citizen and Stratfor's Chief Executive Officer ("CEO").

10. Jurisdiction is proper in this Court pursuant to: a) 28 U.S.C. § 1331, because this case involves a federal question; and b) 28 U.S.C. § 1332(d), because this is a class action lawsuit in which the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one member of the putative class is a citizen of the State of New York, hence a different state than that of the Defendants.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because Plaintiffs reside in this District and a substantial portion of the events and omissions giving rise to this action occurred in this District.

III. Factual Allegations Concerning Plaintiffs David Sterling and Sterling & Sterling

12. Plaintiff Sterling is the CEO of S&S and a Customer of Defendants' Stratfor publication. On December 28, 2011, Sterling received an email from Stratfor with the address: mail@response.stratfor.com. The email was sent to Sterling's S&S email account, the email address that Sterling had provided to Defendants. The email entitled "Important security information from STRATFOR," informed Sterling:

> As we alerted you over the weekend, an unauthorized party illegally obtained and disclosed personally identifiable information and related credit card data of some of our members.
>
> We deeply regret that this event has occurred, and we are working to prevent it from happening again.
>
> Our highest concern is the impact that this has had on you, our loyal members and friends.
>
> As a result and at our expense, we have taken measures to provide our members whose personally identifiable information may have been compromised with access to CSID, a leading provider of global identity protection and fraud detection solutions and technologies.
>
> We have arranged to provide one year of CSID's coverage to you at no cost. Please take advantage of this service. To verify the authenticity of this email and our partnership with CSID, please view this video from our VP of Intelligence, Fred Burton.
>
> In order to activate your Global ID Protector coverage, visit www.csid.com/stratfor to complete a SECURE sign up process.
>
> This process begins by submitting your unique PIN code: [Code omitted]
>
> ***
>
> As part of our ongoing investigation, we have also decided to delay the launching of our website until a thorough review and adjustment by outside experts can be completed.
>
> We expect this to take approximately a week, but it might take longer – please bear with us as we recover from this unfortunate event.
>
> In the meantime, we will not be deterred from doing what we do best: providing our customers with top-notch geopolitical analysis.
>
> Therefore, while our website is being tested we will be sending geopolitical

analysis to our members via email. If you do not wish to have our analytical content emailed to you, click the link at the bottom of this email to manage your email preferences.

***

Sincerely,
George Friedman

13. Sterling was also notified that his account with Amazon, a leading retailer website, had fallen victim to identity theft. An unidentified third-party had used his personal information obtained from Stratfor's security breach in order to create a false account with Amazon that posed as Sterling's account. In order to prevent further attempts by third-parties seeking to use Sterling's identity for unauthorized purposes, Sterling changed his passwords and accounts with online businesses, forums, and other entities.

14. In addition, after the security breach, the unidentified third-party began using Sterling's American Express credit card to Sterling's detriment.

15. Plaintiff Sterling & Sterling, Inc. is a subscriber to Defendants' Stratfor publication. The credit card information and email address stolen during the security breach are S&S's property.

IV. Factual Allegations

16. Stratfor is a subscription-based provider of geopolitical analysis. Stratfor caters to individual and corporate subscribers providing analysis and commentary on international affairs. Unlike traditional news outlets, Stratfor claims to use unique, intelligence-based approaches to gathering information including a combination of open-source monitoring and ane twork of human intelligence sources. Stratfor analysts evaluate events with the objective of simplifying the complexity of international affairs for its targeted intelligent readership. Stratfor claims its reporting is unbiased and not intended to support any ideology.

17. Stratfor has grown its Customer base to nearly one millions content subscribers and

users. Stratfor's subscriber base includes individuals interested in politics and foreign affairs, corporations, government agencies, law enforcement, and military personnel. As a result, Stratfor has access to sensitive financial and personal information on individuals and entities of public interest.

18. In early December, Friedman claims to have received information that Stratfor's website had experienced a security breach. Third-parties were able to obtain Stratfor's Customer credit card information along with personal data. Thereafter, Friedman met with an FBI special agent, who was already aware of the security breach, and informed Friedman that the FBI was investigating the incident. As recounted in Friedman's public letters, the FBI also notified credit card companies of the security breach and provided the credit card companies with lists of compromised cards numbers.

19. Defendants failed to timely disclose to its Customers and the public, some of which sought to conduct business with Defendants after the security breach, that its computer storage systems had experienced a security breach, that it was known that Customers' credit card and other information was stolen, and that Stratfor had no security system in place to defend against current or future attempts by third-parties to access, obtain, and infiltrate its computer storage systems and its Customer's personal and financial information.

20. In a letter dated January 11, 2012, and entitled, "The Hack on Stratfor" Friedman described his "dilemma" in not informing Stratfor's Customers and the public of the security breach as follows:

> From the beginning I faced a dilemma. I felt bound to protect our customers, who quickly had to be informed about the compromise of their privacy. I also felt bound to protect the investigation. That immediate problem was solved when the FBI told us it had informed the various credit card companies and had provided those companies with a list of compromised cards while omitting that it had come from us. Our customers were therefore protected, as the credit card companies knew the

> credit cards and other information had been stolen and could act to protect the customers. We were not compelled to undermine the investigation.[1]

21. Friedman and Stratfor had an obligation to inform its Customers and the public, some which continued to seek to conduct business with Defendants, of the breach of security. Instead Defendants assumed that its Customers' credit card information was secure due to the FBI's notification of credit card companies. Thus, Stratfor determined that its Customers and the public were not entitled to be informed of the security breach. Further, Defendants strategically decided to withhold knowledge of the breach to Customers and the public knowing that Stratfor's computer storage systems were not more secure than they had been when compromised and no party responsible had been caught. Moreover, Defendants understood that even if a Customers' credit card company notified the Customer of the misappropriation, the credit card company would be unable to tell the Customer the source of the breach, depriving the Customer of the ability to take further precautions.

22. Defendants' basis for withholding news of the security breach from Customers and the public was proven wrong when third-parties again targeted Stratfor's computer storage systems. Freidman explained that:

> Early in the afternoon of Dec. 24, I was informed that our website had been hacked again. The hackers published a triumphant note on our homepage saying that credit card information had been stolen, that a large amount of email had been taken, and that four of our servers had been effectively destroyed along with data and backups. We had expected they would announce the credit card theft. We were dismayed that emails had been taken. But our shock was at the destruction of our servers. This attack was clearly designed to silence us by destroying our records and the website, unlike most attacks by such groups.[2]

23. Because those who gained access to Stratfor's servers disclosed to the public that Stratfor's Customers' financial and personal information had been compromised, we will never

---

[1] http://www.stratfor.com/weekly/hack-stratfor (last visited Jan. 20, 2012).
[2] *Id.*

know when, if ever, Defendants would have disclosed the security breach.

24. Indeed, Defendants were strongly motivated to conceal the security breach due to their embarrassment at how easily their systems had been compromised due to the complete absence of security measures to protect such information. Friedman wrote in his letter, "We knew our reputation would be damaged by the revelation, all the more so because we had not encrypted the credit card files. This was a failure on our part."[3]

25. Friedman took full responsibility for the security failure and opined that the "failure originated in the rapid growth of the company. As it grew, the management team and administrative processes didn't grow with it."[4]

26. As a result of Defendants admitted failure to take reasonable steps to secure its payment processing systems, databases, and servers, third parties disclosed financial and personal information including, but not limited to, names, credit card numbers, credit card expiration dates, CVV number, username, passwords, email addresses, phone numbers, and addresses for an estimated 75,000 customers and 860,000 registered users who are now subject to, and have in fact been, used for identity theft, unauthorized credit card charges, and additional cyber-attacks. Amongst the information obtained by third-parties were 19,000 email addresses belonging to the U.S. government's .gov and .mil domains, at least 90,000 credit card accounts and 5.2 million private email communications subject to future disclosure. Information already disclosed and information expected to be leaked in the near future have and will lead to further invasion of privacy of class members, wrongful and malicious use of emails to assist in launching further attacks on the computer systems various entities and individuals alike.

27. In fact, Stratfor has admitted that its Customers have already fallen victim to

[3] *Id.*
[4] *Id.*

additional attempts by third parties to acquire more personal information on its Customers or infect their systems with computer viruses. In a January 6, 2012, email Defendants state:

> While addressing matters related to the breach of Stratfor's data systems, the company has been made aware of false and misleading communications that have circulated within recent days. Specifically, there is a fraudulent email that appears to come from George.Friedman[at]Stratfor.com.
>
> I want to assure everyone that this is not my email address and that any communication from this address is not from me. I also want to assure everyone that Stratfor would never ask customers and friends to provide personal information through the type of attachment that was part of the email at issue. This email, and all similar ones, are false and attempt to prey on the privacy concerns of customers and friends. We strongly discourage you from opening such attachments. We deeply regret the inconvenience this latest development has created.
>
> While Stratfor works to reestablish its data systems and web presence, we ask everyone to please look for official communications, such as this one, and to monitor the Stratfor Facebook page and Twitter feed for company-approved communications.

28. The list of corporations and entities that have had private information taken and already disclosed include BAE Systems Plc, Boeing Co, Lockheed Martin Corp, Bank of America, Exxon Mobil Corp, Goldman Sachs & Co and Thomson Reuters. Several U.S. government-funded labs that conduct classified research in Oak Ridge, Tennessee; Idaho Falls, Idaho; and Sandia and Los Alamos, New Mexico are also included in Stratfor's database. Notable individuals who have had their private information disclosed publicly include, former U.S. Vice President Dan Quayle, former Secretary of State Henry Kissinger and former CIA Director Jim Woolsey.

V. Class Action Allegations

29. Plaintiffs bring this action on behalf of themselves and a Class consisting of all persons, corporations, or entities whose financial and/or personal information was obtained by third-parties due to the breach of Stratfor's computer storage systems. Excluded from the Class are Defendants and its affiliates, parents, subsidiaries, employees, officers, agents, and directors;

government entities or agencies, its affiliates, employees, officers, agents, and directors in their governmental capacities;a ny judicial officer presiding over this matter and the members of their immediate families and judicial staff.

30. Plaintiffs are members of the Class they seek to represent.

31. Upon information and belief, Defendants marketed and advertised to Customers that information provided to Defendants would remain confidential and private implying that reasonable security measures were in place to maintain confidentiality.

32. At all times relevant, Defendants misled Customers that the information provided to Defendants was protected and would remain confidential.

33. Upon information and belief, Plaintiffs and the Class relied upon the Defendants' promises to protect their confidential and private information.

34. Defendants' gross annual sales are approximately $5-10 million. Defendants' sales revenues are believed to be generated through Customer payments to Stratfor.

35. Plaintiffs and the Class have been damaged as a result of Defendants' failure to secure its systems and notify Plaintiffs and the Class of the theft of their personal and financial information causing injuries including:

a. direct financial expenses due to unauthorized use of credit card account information;

b. hassle and expense of securing replacement of compromised credit card numbers, passwords, and employment of monitoring services to protect against fraud;

c. the deprivation of opportunities to safeguard personal and financial information, monitor credit card activity, and take steps to prevent identity theft;

d. losses as a result of computer viruses targeting corporations, individuals, and other entities using email addresses and personal information obtained;

e. Potential disclosure of private email communications; and

f. Loss of use of paid for services on the Stratfor website due to its being incapacitated for 18 days.

36. Defendants are liable to pay to Plaintiffs and the Class monetary, statutory, equitable, and consequential damages for Defendants foregoing acts as well as Plaintiffs' reasonable attorney's fees and costs of suit.

A. Numerosity - Federal Rule of Civil Procedure 23(a)(1)

37. At this time, Plaintiffs do not know the exact size of the Class; however, due to the nature of the trade and commerce involved, Plaintiffs believe that Class members number in the hundreds of thousands if not close to 1 million current and prior subscribers, users, and persons who provided Defendants with personal and financial information and are thus so numerous that joinder of all members is impracticable. The number of class members can be determined through appropriate discovery.

B. Typicality - Federal Rule of Civil Procedure 23(a)(3)

38. Plaintiffs' claims are typical of the claims of the Class because they and all of members of the Class have provided Defendants with personal and financial information and have been comparably injured through Defendants' misconduct as described above and were all subject to Stratfor's security breach.

C. Commonality - Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3)

39. There are numerous common questions of law and fact relative to Plaintiffs and the Class that predominate over any questions affecting Plaintiffs or individual Class members, including but not limited to the following:

a. Whether Defendants failed to use reasonable care and commercially reasonable methods to secure and safeguard its Customers sensitive personal and financial information;

b. Whether Defendants properly implemented security measures to protect Customer personal and financial information from unauthorized capture, dissemination, and misuse;

c. Whether Defendants took reasonable measures to determine the extent of the security breach after it first learned of same;

d. Whether Defendants' delay in informing Customers and the public of the security breach was unreasonable;

e. Whether Defendants' method of informing Customers of the security breach and its description of the breach and potential exposure to damages as a result of same was unreasonable;

f. Whether Defendants' conduct violates the Stored Communications Act, 18 U.S.C. § 2702;

g. Whether Defendants' conduct violates the New York General Business Law §349 or §350.;

h. Whether Defendants' conduct constitutes negligence;

i. Whether Defendants' conduct constitutes breach of contract; and

j. Whether Defendants' conduct constitutes breach of a quasi-contract or an implied-in-law contract; and

k. Whether Plaintiffs and the other members of the Class are entitled to damages or other equitable relief.

40. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

D. Adequacy of Representation - Federal Rule of Civil Procedure 23(a)(4)

41. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class.

42. Plaintiffs have no claims antagonistic to those of the Class.

43. Plaintiffs have retained competent and experienced counsel in complex class actions and consumer actions.

44. Counsel is committed to the vigorous prosecution of this action.

E. Insufficiency of Separate Actions - Federal Rule of Civil Procedure 23(b)(1)

45. Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual Customers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated Customers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Defendants.

F. Superiority – Federal Rule of Civil Procedure 23(b)(3)

46. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if the Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. Given the similar nature of the Class members' claims, class treatment of this litigation will ensure that all claims and claimants are before this

Court for consistent adjudication thereof and will be easily managed by the Court and the parties to this action.

VI. Claims Alleged

COUNT I

Violation of the Federal Stored Communications Act, 18 U.S.C. § 2702

47. Plaintiffs incorporate each of the foregoing allegations as if fully set forth herein.

48. The Stored Communications Act ("SCA") provides consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S.Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, at 3557.

49. Section 2702(a)(2)(A) of the SCA provides "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

50. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

51. An "electronic communications system" is defined by the SCA as "any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

52. Defendants provide remote computing services to the public through online systems that accept user inputs for computer storage and processing services. Defendants store personal and financial information on behalf of the public and utilize such information to process its services on behalf of Customers.

53. Upon information and belief, by failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Defendants knowingly divulged customer names, credit card numbers, credit card expiration dates, CVV number, username, passwords, email addresses, emails, phone numbers, and addresses due to the security breach of their computer storage systems. Further, upon learning that their servers and computer storage systems had been intruded upon and information had been obtained and accessed by third-parties, Defendants failed to safeguard their systems, inform Customers or the public of the security breach, and continued to knowingly divulge Customers information to third-parties.

54. As a result of Defendants conduct described herein and its violations of the SCA, Plaintiffs and the other members of the Class have suffered injuries as described above.

55. Plaintiffs, on their own behalf and on behalf of the other members of the Class, seek judgment in their favor and against Defendants awarding them and the other Class members the maximum statutory damages available under 18 U.S.C. § 2707, including punitive damages for willful or intentional violations.

COUNT II

Deceptive Acts and Practices Under New York General Business Law §349

56. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

57. Upon information and belief, Defendants willfully or knowingly engaged in

deceptive and misleading representations and omissions aimed at deceiving reasonable consumers and the public that Defendants were taking reasonable steps to secure Customers' personal and financial information on their servers and computer storage systems.

58. Defendants advertised to Customers and the public that information submitted, transmitted, and inputted through Defendants' website would be held in confidence and would be reasonably secure against invasion, intrusion, and infiltration by unauthorized parties.

59. As a direct and proximate cause of Defendants' deception to Customers and the public, Plaintiffs and the Class have suffered and continue to suffer harm and damages as described in the foregoing.

60. Defendants are liable to Plaintiffs and the Class for all damages Plaintiffs and the Class suffered and that are available at law.

COUNT III

False Advertising Under New York General Business Law §350

61. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

62. Upon information and belief, Defendants willfully or knowingly engaged in deceptive and misleading representations through false advertisement aimed at deceiving reasonable consumers and the public that Defendants were taking reasonable steps to secure Customers personal and financial information on their servers and computer storage systems.

63. Defendants advertised to Customers and the public that information submitted, transmitted, and inputted through Defendants' website would be held in confidence and would be reasonably secure against invasion, intrusion, and infiltration by unauthorized parties.

64. As a direct and proximate cause of Defendants' deception to Customers and the

public, Plaintiffs and the Class have suffered and continue to suffer harm and damages as described in the foregoing.

65. Defendants are liable to Plaintiffs and the Class for all damages Plaintiffs and the Class suffered that are available at law.

COUNT IV

Breach of Contract

66. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

67. Defendants breached their contract with Plaintiffs and other members of the Class who entered into contracts and a paid subscription fee for Defendants publication and website services.

68. As a result of Defendants security failure, the destruction of Stratfor's servers left the website crippled for nearly three weeks from December 24, 2011 through January 11, 2012 leading to a loss of at least $1.3 million in services Customers paid for but did not receive and thus deprived Plaintiffs and subscribing members of the Class the benefit of their bargain with Defendants due to the Stratfor's security failure.[5]

69. Defendants are liable to Plaintiffs and the Class for all damages Plaintiffs and the Class suffered that are available at law.

COUNT V

Quasi-Contract or
Implied-In-Law Contract

70. Plaintiffs incorporate the allegations within all prior paragraphs within this

[5] This figure assumes a subscriber base of 75,000 customers, a stated retail price of $349 annually, and a loss of service for 18 days.

Complaint as if they were fully set forth herein.

71. Defendants entered into a quasi-contract or alternatively an implied-in-law contract with Plaintiffs and members of the Class to take reasonable steps to protect, hold, and maintain personal and confidential information provided to Defendants.

72. Plaintiffs and members of the Class conferred a benefit upon Defendants by providing Defendants with personal and financial information so as to allow Defendants to contact, transmit billing information, advertise, promote, send email distributions, mail, and engage in commerce or solicit commercial transactions to further Defendants' business interests with respect to Plaintiffs and members of the Class.

73. Defendants impliedly and expressly through use and services provided accepted the corresponding obligation to protect, hold, and maintain personal and confidential information provided to Defendants by Plaintiffs and members of the Class.

74. As a result of Defendants security failure Plaintiffs and members of the Class suffered as a direct and proximate cause the damages described above. Defendants are liable to Plaintiffs and the Class for all just and equitable relief Plaintiffs and the Class suffered.

COUNT VI

Negligence

75. Plaintiffs incorporate the allegations within all prior paragraphs within this Complaint as if they were fully set forth herein.

76. Defendants assumed a duty of care deriving from the nature of services provided, the catastrophic consequences of breach of security, and the nature of the relationship between Plaintiffs and Class members with Defendants. Thus, Defendants were required it to exercise reasonable care to secure and safeguard Plaintiffs' and members of Class' personal and financial

information by agreeing to accept Plaintiffs' and Class members' personal and financial information through its website and storing the information in its computer storage systems.

77. Defendants breached its duty of care by failing to provide reasonable security and by failing to protect Plaintiffs' and the other Class members' personal and financial data from being captured, accessed, disseminated, and misused by third parties.

78. Defendants also breached its duty of care by failing to provide accurate, prompt, and clear notification to Plaintiffs and members of the Class that their personal and financial data had been compromised by unauthorized third-parties.

79. As a direct and proximate result of Defendants failure to exercise reasonable care and use commercially reasonable security measures Defendants were the direct and proximate cause of Plaintiffs' and the other Class members' injuries as described above.

80. Plaintiffs and members of the Class have suffered injury in fact, including money damages, and will continue to incur damages as a result of Defendants negligence.

VII. Request for Relief

WHEREFORE, Plaintiffs request that this Honorable Court enter judgment in their favor and against Defendants and: (1) certify the Class set forth herein; (2) appoint Plaintiffs' Counsel as Class Counsel; (3) award compensatory damages in an amount greater than $50 million; (4) award punitive damages in an amount to be determined at trial; (5) award pre-judgment interest and post-judgment interest on all compensatory and punitive damages; (6) award all costs, expenses and attorneys' fees incurred by Plaintiffs and the Class; and (7) award any and all other relief to which this Court deems Plaintiffs and the Class are justly entitled.

Dated: January 20, 2012
New York, New York

Respectfully submitted,

NAPOLI BERN RIPKA SHKOLNIK, LLP

HUNTER J. SHKOLNIK (HS4854)
ADAM J. GANA (AG1822)
350 Fifth Avenue, Suite 7413
New York, New York 10118
(212) 267-3700 (Phone)
(212) 587-0031 (Fax)
Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

DAVID STERLING, an Individual and STERLING & STERLING,I NC., a corporation on behalf of themselves and others similarly situated,

CIVIL ACTION NO._____

Plaintiffs,

COMPLAINT

v.

STRATEGIC FORECASTING, INC. and GEORGE FRIEDMAN

JURY TRIAL DEMANDED

Defendants.
----------X

SUMMONS AND VERIFIED COMPLAINT

NAPOLI BERN RIPKA SHKOLNIK, LLP
Counsel for: Plaintiffs
350 Fifth Avenue, Suite 7413
New York, New York 10118
(212) 267-3700

The undersigned attorney hereby certifies, pursuant to Fed. R. Civ. P. 11 that I have read the within papers and that to the best of my knowledge and belief they are not frivolous as that term is defined in Fed. R. Civ. P. 11.

Attorney name: Adam J. Gana

PLEASE TAKE NOTICE:

☐ NOTICE OF ENTRY
that the within is a (certified) true copy of an duly entered in the office of the clerk of the within named court on _____ 200__.

☐ NOTICE OF SETTLEMENT
that an order of which the within is a true copy, will be presented for settlement to the HON. one of the judges of the within named Court, at on 200___ at_____ O'clock ___.M.

Dated, _____

Yours, etc.
Napoli Bern Ripka Shkolnik, LLP